Microsoft SC-400 Administrateur de la protection des informations

SYSTÈMES RÉSEAUX ET SÉCURITÉ

Objectifs	A l'issue de la formation, l'apprenant sera capable de : Configurer les stratégies de prévention de la perte de données - Sécuriser les messages dans Microsoft 365 - Décrire le processus de configuration de la gouvernance de l'information - Définir les termes clés associés aux solutions de protection et de gouvernance des informations de Microsoft - Comprendre comment utiliser les types d'informations sensibles et les classificateurs - Passer en revue et analyser les rapports DLP - Identifier et atténuer les violations de la stratégie DLP - Savoir décrire l'intégration de DLP avec Microsoft Cloud App Security (MCAS) - Déployer Endpoint DLP - Décrire la gestion des enregistrements - Comprendre comment configurer la rétention basée sur les événements - Pouvoir importer un plan de fichiers - Savoir configurer les politiques et les étiquettes de rétention - Créer des dictionnaires de mots clés personnalisés - Mettre en œuvre la prise d'empreintes de documents.
Participants	Administrateur et responsable de solutions traditionnelles souhaitant évoluer vers Azure. Tout professionnel de l'informatique s'interrogeant sur Microsoft Azure.
Prérequis	Connaissance de base des technologies de sécurité et de conformité Microsoft - Connaissance de base des concepts de protection des informations - Compréhension des concepts du cloud computing - Compréhension des produits et services Microsoft 365 - Un entretien en amont avec notre expert permet de prendre en compte le profil de chaque participant (niveau, objectifs et résultats attendus, contexte professionnel, enjeux...) et d'adapter le contenu de la formation si besoin.
Moyens pédagogiques	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et Evaluation des acquis tout au long de la formation.
Méthodes pédagogiques	Exposés théoriques et démonstrations. Le formateur évalue la progression pédagogique des apprenants via des QCM et échanges d'expériences Mises en situation et travaux dirigés Accompagnement personnalisé du formateur avec des tests de positionnement.
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants.
Tarif inter-entreprise	2790 € HT
Durée	4 jour(s) - 28 heure(s)

Code : NCI_10OQU2M

Programme :

Comprendre la protection des informations et à la gestion du cycle de vie des données dans Microsoft Purview

Discuter de la protection des informations et de la gestion du cycle de vie des données et de leur importance.

Décrire l'approche de Microsoft en matière de protection des informations et de gestion du cycle de vie des données.

Définir les termes clés associés aux solutions de protection des informations et de gestion du cycle de vie des données de Microsoft.

Identifier les solutions qui comprennent la gestion du cycle de vie des informations et des données dans Microsoft Purview.

Classifier les données pour la protection et la gouvernance

Répertorier les composants de la solution Data Classification.

Identifier les cartes disponibles dans l'onglet Vue d'ensemble de la classification des données.

Utiliser l'explorateur de contenu et l'explorateur d'activités.

Utiliser les types d'informations sensibles et les classificateurs pouvant être entraînés.

Créer et gérer des types d'informations sensibles

Différencier les étiquettes de confidentialité intégrées et les personnalisées.

Configurer des types d'informations sensibles avec une classification exacte basée sur des correspondances de données.

Implémenter l'identification par empreinte de document. Créer des dictionnaires de mots clés personnalisés.

Comprendre le cryptage de Microsoft 365

Atténuer le risque de divulgation non autorisée de données grâce au cryptage.

Décrire les solutions de chiffrement des données au repos et en transit de Microsoft.

Mettre en œuvre le cryptage des services pour protéger les données des clients au niveau de la couche applicative.

Différencier les clés gérées par Microsoft et les clés gérées par le client pour l'utilisation du cryptage des services.

Déployer le chiffrement des messages Microsoft Purview

Configurer le Chiffrement de messages Microsoft Purview pour les utilisateurs finaux. - Implémenter le Chiffrement avancé des messages Microsoft Purview.

Créer et configurer des étiquettes de sensibilité avec Microsoft Purview

Comprendre les bases des étiquettes de sensibilité Microsoft Purview dans Microsoft 365.

Créer et publier des étiquettes de sensibilité pour classer et protéger les données.

Configurer les paramètres de cryptage avec des étiquettes de sensibilité pour une sécurité améliorée des données.

Mettre en œuvre l'étiquetage automatique pour une classification et une protection cohérente des données.

Utiliser le tableau de bord de classification des données Microsoft Purview pour surveiller l'utilisation des étiquettes de sensibilité.

Appliquer des étiquettes de confidentialité pour la protection des données

Appliquer des étiquettes de confidentialité à Microsoft Teams, des groupes Microsoft 365 et des sites SharePoint.

Surveiller l'utilisation des étiquettes à l'aide de l'analytique d'étiquette.

Configurer un étiquetage local.

Gérer les paramètres de protection et le marquage des étiquettes de confidentialité appliquées.

Appliquer des protections et des restrictions à des e-mails.

Appliquer des protections et des restrictions à des fichiers.

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon

Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille

www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20